

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: John Owlett

Serial No.: 10/081,500

Filed: February 22, 2002

For: METHOD AND SYSTEM FOR AUTHENTICATION OF A USER

Confirmation No.: 1505

Group No.: 2131

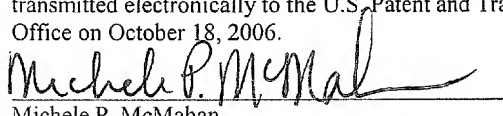
Examiner: Christian A. LaForgia

Date: October 18, 2006

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**CERTIFICATION OF ELECTRONIC TRANSMISSION
UNDER 37 CFR § 1.8**

I hereby certify that this correspondence is being
transmitted electronically to the U.S. Patent and Trademark
Office on October 18, 2006.


Michele P. McMahan

APPELLANT'S REPLY BRIEF ON APPEAL UNDER 37 C.F.R. §41.41

Sir:

This Reply Brief is filed in response to the Examiner's Answer mailed September 19, 2006.

It is not believed that an extension of time and/or additional fee(s) are required, beyond those that may otherwise be provided for in documents accompanying this paper. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned for under 37 C.F.R. §1.136(a). Any additional fees believed to be due in connection with this paper may be charged to Deposit Account No. 09-0457.

II. The Examiner's Answer – Response to Arguments (starting at Page 10)

Appellant will refrain from readdressing all of the deficiencies with the pending rejections herein. In the interest of brevity, Appellant will only address new arguments made in the Examiner's Answer. Accordingly, Appellant hereby incorporates herein the arguments set out in Appellant's Brief on Appeal as if set forth in their entirety.

A. Claims 1, 13, and 14

The Examiner's Answer first argues that features upon which Appellant's arguments rely are not recited in the rejected claims. *See* Examiner's Answer, page 6-7. Specifically, the Examiner's Answer states that "security benefits of a spoiler" and "a spoiler function" are not recited in the rejected claims. Examiner's Answer, page 6-7. The Examiner's Answer misinterprets Appellant's arguments. Appellant's argument is, in short, that Hara does not disclose or suggest **"adding a spoiler"** to the challenge; encrypting the **combined spoiler and challenge** using a private key of an asymmetric key pair and sending a response to the authenticating entity **in the form of the encrypted combined spoiler and challenge**" as recited in Claim 1.

Appellant's arguments provide discussion of the security benefits of a spoiler as evidence that "a spoiler" is distinctive from padding data disclosed in Hara. Hara discloses adding padding bits all valued at "1" to make the length of the data part an integer multiple of 64. *See* Hara, paragraph 83. One of ordinary skill in the art would recognize that an encryption algorithm can be actually weakened when a portion of the original data is predetermined and known to others. In contrast, "a spoiler" includes additional bits (1's and 0's), not always 1's, and therefore is not as easy to predict. Thus, the presence of the spoiler can strengthen the security of the encryption, thereby adding security benefit. Again, padding data, as disclosed in Hara, is not a "spoiler," as recited in Appellant's claims. Appellant respectfully submits that nothing in Hara discusses the addition of a "spoiler" as recited in Claims 1, 13, and 14 for at least these additional reasons.

Accordingly, in response to Appellant's arguments that the spoiler adds a level of security, the Examiner's Answer states:

[A] recitation of intended use of the claims invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

See Examiner's Answer, page 7. The Examiner's Answer erroneously concludes that padding data is capable of performing the intended use of a spoiler. As discussed above, a spoiler is distinctive from padding data in its intended use. Padding data is merely a placeholder having a known and fixed value for any given number of fill bits required to achieve dimensionally

convenient data. In contrast, a spoiler can have a variety of values, the quantity of which is limited only by bit-length. The variety of available values provides security benefits that fixed value padding data may not provide. Thus, a spoiler and padding data are different in kind as they serve different purposes. Furthermore, the intended uses of padding data and a spoiler are not interchangeable. For example, if padding data were used instead of a spoiler in the context of Appellant's invention, some of Appellant's advantageous features would be rendered non-functional. Thus, the spoiler is distinctive from the padding data in kind and intended use. In contrast with padding data always having the same value, as disclosed in Hara, the spoiler value is defined by a user and, in some embodiments, must be shared with another user for the purposes of decrypting a communication. *See e.g.*, Appellant's Specification, lines 1-3. Accordingly, Claims 1, 13, and 14 are patentable for at least these additional reasons.

The Examiner's Answer further argues that the Appellant defines a spoiler as "be[ing data] added to the challenge as a prefix or a suffix and the authenticating entity extracts the challenge by counting the number of bytes from the beginning or end of the combined spoiler and challenge." *See* Examiner's Answer, page 7. Appellant respectfully submits that the language cited in the Examiner's Answer is provided in the Summary and describes one embodiment discussing how a spoiler can be added to/extracted from the data. Thus, the cited portion of the specification does not define a spoiler as recited in the claims.

The Examiner's Answer further argues that Hara provides a motivation to combine the references in suggesting that "adding padding information, or a spoiler, to data makes it better suited for encryption." Examiner's Answer, page 8. Appellant disagrees for various reasons. The Examiner's Answer incorrectly suggests that padding data is synonymous with a spoiler. As Appellants have discussed, this is clearly not the case. Furthermore, the Examiner's Answer appears to suggest that "better suited for encryption" results in improved security, when, in fact, the "better suited for encryption" appears to be in reference system data transmission characteristics. For example, Hara discusses:

With the destination address thus found out, the data transmitter 2 creates a section in accordance with the destination address. At this point, the data transmitter 2 provides the data part with bit "1" padding as needed so that the data part will become a multiple of 64 bits.

See Hara, paragraph 128. As stated by Hara, the padding data is added merely to achieve a specific data part size. Appellant respectfully submits that Claims 1, 13, and 14 are patentable over the cited references for at least the additional reasons discussed herein.

The Examiner's Answer appears to justify the hindsight reasoning as properly used in the rejection of these claims. The Examiner's Answer states:

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such reconstruction is proper. *See In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

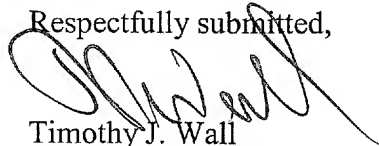
See Examiner's Answer, page 8. In this response, the Examiner's Answer appears to do no more than justify the hindsight reasoning used in the rejection by reciting old case law. Numerous examples of case law in the thirty-five years since 1971 serve to provide additional guidance regarding the motivation to combine references. Appellant respectfully submits that as a general principle the case law is clear that the motivation to combine must be clear and particular. *See, e.g. Winner International Royalty Corp. v. Wang*, 202 F.3d 1340, 53 U.S.P.Q.2d 1580, 1587, (Fed. Cir. 2000). Regarding the use of hindsight, "one cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention." *In re Fritch*, 792 F.2d 1260, 23 U.S.P.Q.2d 1780, 1784 (Fed. Cir. 1992).

If the motivation provided by the Examiner were adequate, then any modification that would modify data as part of a communication and/or encryption scheme would be obvious. This cannot be the standard. The Examiner cannot just locate each of the recitations of the claims in two or more references, combine them, and then justify the combination by merely stating that every combination includes hindsight. The motivation to combine references must be obvious (clear and particular) without using Appellant's disclosure as a roadmap. Accordingly, Appellant respectfully submits that Claims 1, 13, and 14 are patentable for at least these additional reasons.

III. Conclusion

For the reasons set forth in above and in Appellant's Brief on Appeal, Appellant requests reversal of the rejections of the claims, allowance of the claims and passing of the application to issue.

Respectfully submitted,



Timothy J. Wall
Registration No. 50,743

Customer No. 46590

Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401